*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**
**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**
**http://www.us-cert.gov/tlp/**

**DATE(S) ISSUED:**
05/17/2016

**SUBJECT:**
Multiple Vulnerabilities in Apple Products Could Allow For Arbitrary Code Execution

**OVERVIEW:**
Multiple vulnerabilities have been discovered in iOS, watchOS, tvOS, iTunes, OS X El Capitan, and Safari which could allow for arbitrary code execution. Apple iOS is an operating system for iPhone, iPod touch, and iPad. watchOS is the mobile operating system of the Apple Watch. tvOS is an operating system for Apple TV digital media player. Apple iTunes is used to play media files on Microsoft Windows and MAC OS X platforms. OS X El Capitan is an operating system for Macintosh computers. Apple Safari is a web browser available for OS X and Microsoft Windows.

Successful exploitation of these vulnerabilities could result in, but are not limited to information disclosure, giving an attacker the ability determine kernel memory layout, or allow for arbitrary code to be run within the context of the user or kernel.

**THREAT INTELLIGENCE:**
There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEMS AFFECTED:**
- tvOS prior to 9.2.1 for Apple TV (4th generation)
- iOS prior to 9.3.2 for iPhone 4s and later, iPod touch (5th generation) and later, and iPad 2 and later
- watchOS prior to 2.2.1 for Apple Watch Sport, Apple Watch, Apple Watch Edition, and Apple Watch Hermes
- OS X El Capitan prior to v10.11.5 and Security Update 2016-003 for OS X El Capitan v10.11and later
- Safari prior to 9.1.1 for OS X Mavericks v10.9.5, OS X Yosemite v10.10.5, and OS X El Capitan v10.11.5
- iTunes prior to 12.4 for Windows 7 and later

**RISK:**
**Government:**
- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**
- Large and medium business entities: **High**

- Small business entities: **Medium**

**Home users: Low**

**TECHNICAL SUMMARY:**

Multiple vulnerabilities have been discovered in iOS, watchOS, tvOS, iTunes, OS X El Capitan, and Safari. The most serious of these vulnerabilities could lead to arbitrary code execution. Details of all vulnerabilities are as follows:

- Clear History and Website Data did not clear the history. The issue was addressed through improved data deletion (CVE-2016-1849).
- An insufficient taint tracking issue in the parsing of svg images was addressed through improved taint tracking (CVE-2016-1858).
- Multiple memory corruption issues were addressed through improved memory handling (CVE-2016-1792, CVE-2016-1795, CVE-2016-1804, CVE-2016-1810, CVE-2016-1815, CVE-2016-1817, CVE-2016-1818, CVE-2016-1819, CVE-2016-1822, CVE-2016-1823, CVE-2016-1824, CVE-2016-1825, CVE-2016-1827, CVE-2016-1828, CVE-2016-1829, CVE-2016-1830, CVE-2016-1831, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-1841, CVE-2016-1846, CVE-2016-1847, CVE-2016-1848, CVE-2016-1850, CVE-2016-1854, CVE-2016-1855, CVE-2016-1856, CVE-2016-1857, CVE-2016-1859).
- A memory corruption issue existed in the parsing of disk images. This issue was addressed through improved memory handling (CVE-2016-1808).
- Multiple memory corruption issues were addressed through improved input validation (CVE-2016-1799, CVE-2016-1832).
- A memory corruption vulnerability was addressed through improved locking (CVE-2016-1819).
- A dynamic library loading issue existed in iTunes setup. This was addressed through improved path searching (CVE-2016-1742).
- An issue existed that led to the disclosure of kernel memory content. This issue was addressed through improved bounds checking (CVE-2016-1791).
- Multiple vulnerabilities existed in PHP versions prior to 5.5.34. These were addressed by updating PHP to version 5.5.34 (CVE-2015-8865, CVE-2016-3141, CVE-2016-3142, CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073).
- Multiple null pointer dereferences were addressed through improved validation (CVE-2016-1793, CVE-2016-1794, CVE-2016-1798, CVE-2016-1803, CVE-2016-1811, CVE-2016-1813, CVE-2016-1816, CVE-2016-1821).
- A null pointer dereference was addressed through improved locking (CVE-2016-1814).
- An out of bounds memory access issue was addressed through improved memory handling (CVE-2016-1796).
- An issue existed in the sandbox policy. This was addressed by sandboxing FontValidator (CVE-2016-1797).
- A custom URL scheme handling issue was addressed through improved input validation (CVE-2016-1800).
- An information leak existed in the handling of HTTP and HTTPS requests. This issue was addressed through improved URL handling (CVE-2016-1801).
- An issue existed in the handling of return values in CCCrypt. This issue was addressed through improved key length management (CVE-2016-1802).
- Multiple configuration issues were addressed through additional restrictions (CVE-2016-1805, CVE-2016-1806).

- A race condition was addressed through improved locking (CVE-2016-1807).
- Incorrect keys were being used to encrypt disk images. This issue was addressed by updating the encryption keys (CVE-2016-1809).
- Multiple buffer overflow vulnerabilities were addressed through improved bounds checking (CVE-2016-1812, CVE-2016-1820).
- A buffer overflow was addressed through improved size validation (CVE-2016-1790).
- An integer overflow existed in dtrace. This issue was addressed through improved bounds checking (CVE-2016-1826).
- Shared links were sent with HTTP rather than HTTPS. This was addressed by enabling HTTPS for shared links (CVE-2016-1842).
- A validation issue existed in roster changes. This issue was addressed through improved validation of roster sets (CVE-2016-1844).
- An encoding issue existed in filename parsing. This issue was addressed through improved filename encoding (CVE-2016-1843).
- An issue existed in the management of password profiles. This issue was addressed through improved password reset handling (CVE-2016-1851).
- A protocol security issue was addressed by disabling SSLv2 (CVE-2016-1853).
- A state management issue existed when accessing Siri results on the lock screen. This issue was addressed by disabling data detectors in Twitter results when the device is locked (CVE-2016-1852).

Successful exploitation could result in an attacker gaining the same privileges as the logged on user, arbitrary code execution within the context of the application, or the ability to bypass the security system. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**
The following actions should be taken:
- Apply appropriate updates provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

**REFERENCES:**
https://support.apple.com/en-us/HT206379
https://support.apple.com/en-us/HT206564
https://support.apple.com/en-us/HT206565
https://support.apple.com/en-us/HT206566
https://support.apple.com/en-us/HT206567
https://support.apple.com/en-us/HT206568

**CVE:**
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8865
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1742
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1790
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1791

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1792
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1793
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1794
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1795
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1796
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1797
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1798
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1799
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1800
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1801
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1802
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1803
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1804
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1805
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1806
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1807
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1808
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1809
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1810
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1811
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1812
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1813
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1814
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1815
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1816
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1817
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1818
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1819
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1820
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1821
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1822
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1823
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1824
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1825
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1826
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1827
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1828
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1829
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1830
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1831
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1832
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1833
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1834
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1835
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1836
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1837
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1838
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1839

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1840
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1841
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1842
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1843
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1844
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1846
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1847
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1848
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1849
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1850
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1851
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1852
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1853
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1854
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1855
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1856
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1857
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1858
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1859
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3141
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3142
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4070
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4071
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4072
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4073